Sekhmet

id-ransomware.blogspot.com/2020/03/sekhmet-ransomware.html

Sekhmet Ransomware

Sekhmet Doxware

(шифровальщик-вымогатель, публикатор) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей и компаний с помощью RSA-2048 + ChaCha, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. Хакеры-вымогатели: Twisted Spider Extortion Group. Среди вымогателей есть граждане Украины, по другим данным это международная хакерская группа.

Вымогатели, распространяющие **Sekhmet**, угрожают опубликовать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — публикатор). Как известно из других Ransomware, для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов. Об этих акциях вымогателей сообщалось в СМИ. На момент публикации статьи, не было известно о публикациях украденных данных, вымогатели только угрожали, что данные будут опубликованы на их специальном сайте. Потом они создали специальный сайт "Leaks leaks and leaks" для таких публикаций.

Обнаружения:
DrWeb -> Trojan.Encoder.31322, Trojan.Encoder.32301
BitDefender -> Trojan.GenericKD.42872102, Gen:Variant.Jatif.1394
ESET-NOD32 -> A Variant Of Generik.GYISLCY, A Variant Of Win32/Kryptik.HEDE
Malwarebytes -> Trojan.MalPack, Ransom.Sekhmet
Rising -> Ransom.Cryptor!8.10A9 (CLOUD)
Symantec -> Ransom.Gen

TrendMicro -> Ransom.Win32.SEKHMET.A, TROJ_GEN.R002C0RH720

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: Maze > Sekhmet > Egregor

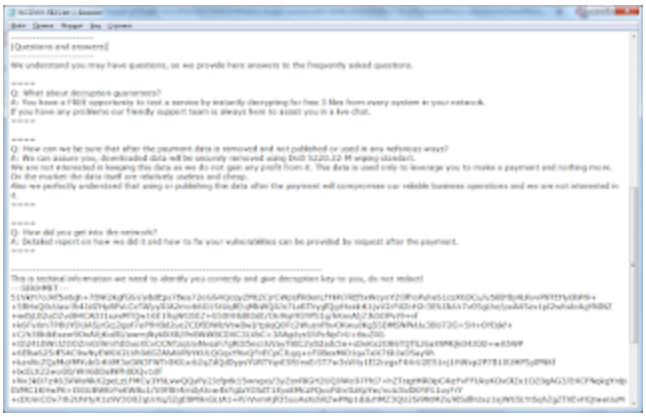
Изображение — логотип статьи

К зашифрованным файлам добавляются разные случайные расширения. например:
.cSlFg
.RXfbY
.jHXeqt
.DtiM
.wlxVM

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на середину марта 2020 г.
Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **RECOVER-FILES.txt**



Содержание записки о выкупе:

| Attention! |

Your company network has been hacked and breached. We downloaded confidential and private data.
In case of not contacting us in 3 business days this data will be published on a special website available for public view.
Also we had executed a special software that turned files, databases and other important data in your network into an encrypted state using RSA-2048 and ChaCha algorithms.

A special key is required to decrypt and restore these files. Only we have this key and only we can give it to you with a reliable decryption software.

| How to contact us and be safe again |

The only method to restore your files and be safe from data leakage is to purchase a private key which is unique for you and securely stored on our servers.
After the payment we provide you with decryption software that will decrypt all your files, also we remove the downloaded data from your network and never post any information about you.
There are 2 ways to directly contact us:
1) Using hidden TOR network:
  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR browser
  c) Open our website in the TOR browser:
xxxx://o3n4bhhtybbtwqqs.onion/C4BA3647FD0D6918
  d) Follow the instructions on this page.
2) If you have any problems connecting or using TOR network
  a) Open our website: xxxxs://sekhmet.top/C4BA3647FD0D6918
  b) Follow the instructions on this page
On this web site, you will get instructions on how to make a free decryption test and how to pay.
Also it has a live chat with our operators and support team.

|Questions and answers|

We understand you may have questions, so we provide here answers to the frequently asked questions.
====
Q: What about decryption guarantees?
A: You have a FREE opportunity to test a service by instantly decrypting for free 3 files from every system in your network.
If you have any problems our friendly support team is always here to assist you in a live chat.
====
====
Q: How can we be sure that after the payment data is removed and not published or used in any nefarious ways?
A: We can assure you, downloaded data will be securely removed using DoD 5220.22-M wiping standart.
We are not interested in keeping this data as we do not gain any profit from it. This data is used only to leverage you to make a payment and nothing more.
On the market the data itself are relatively useless and cheap.

Also we perfectly understand that using or publishing this data after the payment will compromise our reliable business operations and we are not interested in it.
====
====
Q: How did you get into the network?
A: Detailed report on how we did it and how to fix your vulnerabilities can be provided by request after the payment.
====

This is techinal information we need to identify you correctly and give decryption key to you, do not redact!
---SEKHMET---
51VkH7oJKf5e6gh+7BW2KgfGSr/yibdEps7Bea72oGS***BPAFUAUAAAAA== [всего 2504 знака]
---SEKHMET---

Перевод записки на русский язык:

| Внимание! |

Сеть вашей компании была взломана и нарушена. Мы загрузили конфиденциальные и личные данные.
В случае, если нет контакта с нами в течение 3 рабочих дней, эти данные будут опубликованы на специальном веб-сайте, доступном для всеобщего обозрения.
Также мы запустили специальную программу, которая преобразовала файлы, базы данных и другие важные данные в вашей сети в зашифрованное состояние с использованием алгоритмов RSA-2048 и ChaCha.
Специальный ключ нужен для расшифровки и восстановления этих файлов. Только у нас есть этот ключ, и только мы можем дать его вам с надежной программой для расшифровки.

| Как с нами связаться и снова быть в безопасности |

Единственный способ восстановить ваши файлы и обезопасить себя от утечки данных - это приобрести закрытый ключ, который является уникальным для вас и надежно хранится на наших серверах.
После оплаты мы предоставляем вам программу для расшифровки, которая расшифрует все ваши файлы, а также мы удалим загруженные данные из вашей сети и никогда не публикуем информацию о вас.
Есть два способа связаться с нами напрямую:
1) Использование скрытой сети TOR:
  а) Загрузите специальный браузер TOR: https://www.torproject.org/
  б) Установите браузер TOR

c) Откройте наш веб-сайт в браузере TOR:
xxxx://o3n4bhhtybbtwqqs.onion/C4BA3647FD0D6918
г) Следуйте инструкциям на этой странице.
2) Если у вас возникли проблемы с подключением или использованием сети TOR
а) Откройте наш веб-сайт: xxxxs://sekhmet.top/C4BA3647FD0D6918
б) Следуйте инструкциям на этой странице
На этом веб-сайте вы получите инструкции о том, как сделать бесплатную тест-расшифровку и как оплатить.
Также есть живой чат с нашими операторами и службой поддержки.

| Вопросы и ответы |

Мы понимаем, что у вас могут возникнуть вопросы, поэтому мы даем здесь ответы на часто задаваемые вопросы.
====
Q: Как насчет гарантий дешифрования?
O: У вас есть БЕСПЛАТНАЯ возможность протестировать сервис, мгновенно расшифровав бесплатно 3 файла из каждой системы в вашей сети.
Если у вас есть какие-либо проблемы, наша дружная команда поддержки всегда здесь, чтобы помочь вам в чате.
====
====
B: Как мы можем быть уверены, что после того, как платежные данные будут удалены, а не опубликованы или использованы какими-либо гнусными способами?
A: Мы можем заверить вас, загруженные данные будут надежно удалены с использованием стандарта очистки DoD 5220.22-M.
Мы не заинтересованы в сохранении этих данных, поскольку мы не получаем никакой прибыли от них. Эти данные используются только для того, чтобы вы могли совершить платеж и ничего более.
На рынке сами данные относительно бесполезны и дешевы.
Также мы прекрасно понимаем, что использование или публикация этих данных после оплаты поставит под угрозу наши надежные деловые операции, и мы не заинтересованы в них.
====
====
Q: Как вы попали в сеть?
A: Подробный отчет о том, как мы это сделали и как исправить ваши уязвимости, может быть предоставлен по запросу после оплаты.
====
---------- ----------
Это техническая информация, которая нам нужна, чтобы правильно идентифицировать вас и дать вам ключ расшифровки, не редактируйте!

---SEKHMET---
51VkH7oJKf5e6gh+7BW2KgfGSr/yibdEps7Bea72oGS***BPAFUAUAAAAA== [всего 2504 знака]
---SEKHMET---

Содержание официального сайта вымогателей:
WAKE UP SAMURAI!
If you've come to this page, don't waste your time searching for how to solve this problem and do not try to entrust the solution to third parties.
Upload the ransom note RECOVER-FILES.txt and We will tell you how to quickly and reliably recover all your files.

Перевод текста на русский язык:
Проснись Самурай!
Если вы зашли на эту страницу, не тратьте свое время на поиски решения этой проблемы и не пытайтесь доверить решение третьим лицам.
Загрузите записку с требованием выкупа RECOVER-FILES.txt, и мы расскажем вам, как быстро и надежно восстановить все ваши файлы.

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ Для обеспечения запуска используется Regsvr32 — это служебная программа командной строки для регистрации и отмены регистрации элементов управления OLE, например ActiveX и библиотеки DLL в реестре Windows.
Запуск обеспечивается с помощью следующей команды:
"C:\Windows\System32\regsvr32.exe" /s sekhmet.dll.exe

Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
RECOVER-FILES.txt - название файла с требованием выкупа
sekhmet.dll.{exe} - исполняемый файл Ransomware
<random>.exe - случайное название вредоносного файла

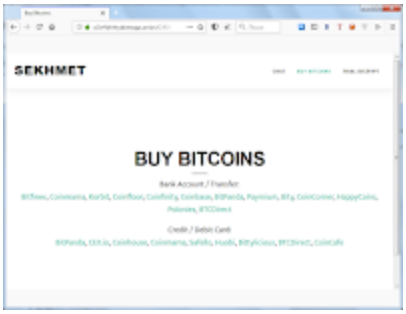
Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
G:\aaaa\bbbb\cccc\dddd\eeee.pdb

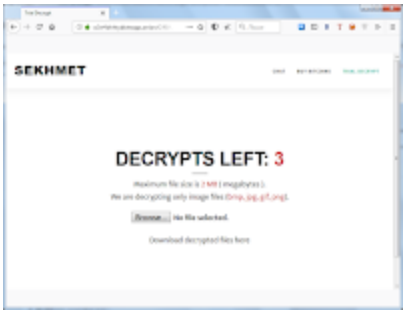
Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
URL: hxxxs://sekhmet.top/
URL: hxxxs://sekhmet.top/C4BA3647FD0D6918

Tor-URL: hxxx://o3n4bhhtybbtwqqs.onion/C4BA3647FD0D6918





Email: -
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ **Hybrid analysis >>**
Σ VirusTotal analysis >>
🐞 **Intezer analysis >>**
⋟ ANY.RUN analysis >>
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

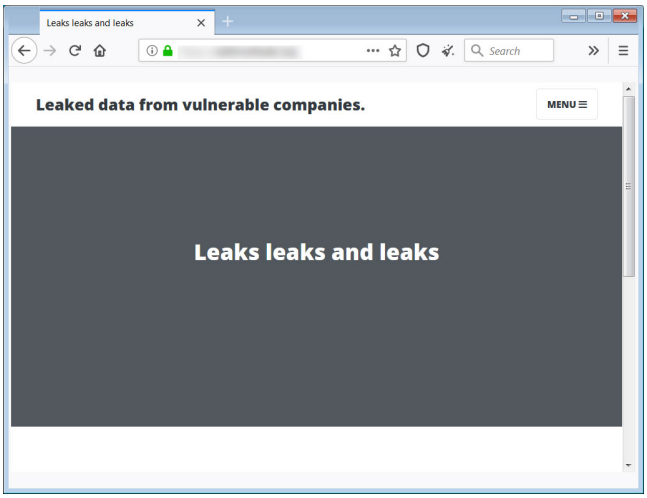
Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

Maze Ransomware - май 2019 - ноябрь 2020
Sekhmet Ransomware - март 2020 - октябрь 2020
Egregor Ransomware - сентябрь 2020 - февраль 2021

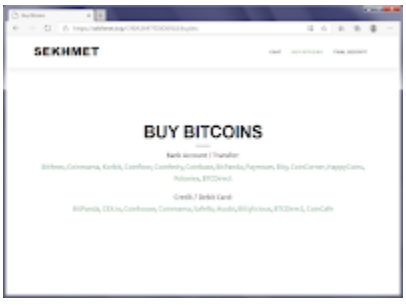
=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Обновление от 24 марта 2020:
Вымогатели создали сайт "Leaks leaks and leaks" для публикаций украденных данных тех компаний, которые отказались платить им выкуп.
Статья на сайте BleepingComputer >>



Обновление от 7-9 августа 2020:
Пост в Твиттере >>
Расширения: **.xgVWib**, **.UQgH**
Записка: RECOVER-FILES.txt

Tor-URL: hxxx://o3n4bhhtybbtwqqs.onion/C4BA3647FD0D6918
URL: hxxxs://sekhmet.top/C4BA3647FD0D6918
Файл: KB083486A.msi - **VT** + **IA** + **AR**
Файл: patch_may13869.dll - **VT** + **IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.32301
BitDefender -> Gen:Variant.Jatif.1394
ESET-NOD32 -> A Variant Of Win32/Kryptik.HEDE
Malwarebytes -> Ransom.Sekhmet
Kaspersky -> Trojan-Ransom.Win32.Cryptor.dox
TrendMicro -> TROJ_GEN.R002C0RH720



➤ Содержание сайта (срок уплаты выкупа истек):

SEKHMET

Price for recovering your files should be negotiated
That means we will provide you the amount after consensus is reached.
Let's start a constructive dialogue.
Looks like you were banned from the chat.
It is the time to reconsider your position and start again.
Check this page later, maybe we will unban you.

BUY BITCOINS

Bank Account / Transfer:
Bitfinex, Coinmama, Korbit, Coinfloor, Coinfinity, Coinbase, BitPanda, Paymium, Bity, CoinCorner, HappyCoins, Poloniex, BTCDirect
Credit / Debit Card:
BitPanda, CEX.io, Coinhouse, Coinmama, Safello, Huobi, Bittylicious, BTCDirect, CoinCafe

---

DECRYPTS LEFT: 0

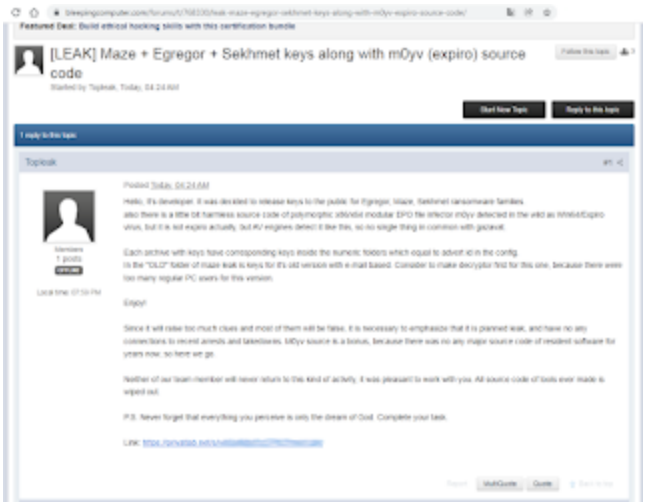
Maximum file size is 2 MB (megabytes).
We are decrypting only image files (bmp, jpg, gif, png).
No more decrypts left.
Download decrypted files here
Error incorrect magic: 2139205805 file is probably not encrypted or encrypted with other software
Error incorrect magic: 1212537294 file is probably not encrypted or encrypted with other software
Error incorrect magic: 2139205805 file is probably not encrypted or encrypted with other software

Обновление от 29 октября 2020:

Статья о закрытии вымогательского проекта "Maze Ransomware" и переход операторов вымогателей на "Egregor Ransomware".
Вымогатели также подтверждили, что Maze, Sekhmet, Egregor являются их вымогательскими программами.

Более того, пострадавшие от Egregor после уплаты выкупа получают Sekhmet Decryptor.
=== 2022 ===

Новость от 9 февраля 2022
Представитель группы вымогателей выложил в общий доступ на форуме BleepingComputer ключи дешифрования для пострадавших от Maze, Sekhmet, Egregor Ransomware.
Ссылка на скриншоте скрыта, чтобы не дать возможность использовать вредоносные файлы инфектора m0yv, которые были в архиве.



Внимание!
Теперь есть дешифровщик >>
Скачайте Emsisoft Decryptor for Maze/Sekhmet/Egregor >>

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===

Thanks:

dnwls0719, Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples